AFFIDAVIT OF SPECIAL AGENT JOHN P FARLEY IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent John P Farley, being sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am an investigative or law enforcement officer of the United States, within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code. I have been a Special Agent with the Federal Bureau of Investigation (FBI) since 2009. I am currently assigned to the FBI, Boston Field Office and have been engaged in gang and drug investigations. Based on my training and experience as a Special Agent, I am familiar with federal narcotics laws. In this regard, I know that it is a violation of 21 U.S.C. §§ 841 and 846 to possess with intent to distribute, distribute, and to conspire to possess with intent to distribute and to distribute controlled substances, including cocaine, cocaine base, and fentanyl. I also know that it is a violation of Title 18 U.S.C. § 922(g)(1) to be a prohibited person in possession of a firearm and ammunition.

2. In the course of participating in drug trafficking investigations, I have conducted or participated in surveillance, the purchase of illegal drugs, the execution of search warrants, interviews of subjects, witnesses, and informants, and reviews of consensually recorded conversations and meetings. I have also received training through my position as an FBI Special Agent regarding drug trafficking. Through my training, education, and experience, I have become familiar with the manner in which drug traffickers conduct their illegal drug trafficking activity, including their use of cellular telephones to contact drug customers, drug runners, drug

associates, and sources of illegal drug supply. I am familiar with narcotics traffickers' methods of operation, including distribution, storage, and transportation of narcotics and laundering of drug proceeds.

3. Based upon my training and experience, I am familiar with narcotics traffickers' (this includes the members and associates of street gangs who distribute narcotics) methods of operation, including the distribution, storage, and transportation of narcotics and the collection of money that constitutes the proceeds of narcotics trafficking activities. Specifically, I am familiar with the manner in which narcotics traffickers use vehicles, common carriers, mail and private delivery services, and a variety of other means to transport and distribute narcotics and the proceeds of narcotics trafficking. I also am familiar with the manner in which narcotics traffickers use telephones, coded or slang-filled telephone conversations, text messages, pagers, coded pager messages, social media, and other means to facilitate their illegal activities. I also am familiar with the vernacular of users and distributors of controlled substances and the methods by which such persons attempt to disguise the subjects of their conversations and operations.

4. I am currently investigating JERRY GRAY ("GRAY"), DOB: xx/xx/1996, and others yet known, for violations of federal law, including Title 21 U.S.C. § 841(a)(1) (possession with intent to distribute, and distribution of, controlled substances) and Title 18 U.S.C. § 922(g)(1) (being a felon in possession of a firearm and ammunition) (the "TARGET OFFENSES").

5. This affidavit is being submitted in support of an application for a warrant to search GRAY's residence;

a. 28 Deckard Street, Apt #6, Roxbury, MA (the "TARGET LOCATION")

6. There is probable cause to believe that the TARGET LOCATION, as described in Attachment A, contains evidence, fruits, and instrumentalities of the crimes listed above, as described in Attachment B.

7. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested search warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED

I. Background

8. Since 2021, the Drug Enforcement Administration Boston Office and the Boston Police Department, with assistance by the FBI, have been investigating the drug distribution activities of members and associates of the "H-Block" criminal street gang, which operates in and around the greater Boston, Massachusetts area, particularly the area of Humboldt Avenue in Roxbury, including Trea LANKFORD ("LANKFORD"), Dennis WILSON ("WILSON"), Avery LEWIS ("LEWIS"), Eric CELESTINO ("CELESTINO"), Mark LINNEHAN ("LINNEHAN"), Robert HECKSTALL ("HECKSTALL"), Dominique CARPENTER-GRADY ("CARPENTER-GRADY"), Jason BLY ("BLY"), Timothy HEARNS ("HEARNS"), Natasha SIERRA ("SIERRA"), Jeremy HARRIS ("HARRIS"), Tony LATTIMORE ("LATTIRMORE"), Randall VARISTE-SCOTT ("VARISTE-SCOTT"), Khamonie MCCALOP ("MCCALOP") and their co-conspirators, known and unknown (collectively, the "Target Subjects").

9. As set forth in affidavits in support of prior applications in this investigation, an undercover DEA TFO (hereinafter, "UC-2") was introduced to LANKFORD for the purpose of purchasing cocaine in October 2021. Thereafter, UC-2 conducted over 20 undercover purchases of cocaine, cocaine base, and fentanyl from LANKFORD and co-conspirators, including but not limited to LEWIS, WILSON, VARISTE-SCOTT, and LINNEHAN. Investigators later initiated four rounds of federal court ordered title III interceptions, which led to the identification of additional conspirators and the seizure of narcotics.

10. In February 2024, investigators utilized an FBI cooperating witness ("CW-1") [1] to conduct a controlled purchase of cocaine from GRAY. 2 In March 2024, investigators attempted a second controlled purchase of cocaine from GRAY, however, GRAY stole the Official Agency Funds from CW-1 during the controlled purchase.

11. On August 21, 2024, a federal grand jury sitting in Boston, Massachusetts returned an indictment (24-cr-10254-AK) charging GRAY with a drug trafficking violation of 21 U.S.C. § 841(a)(1). An arrest warrant for GRAY was issued in connection with the indictment on August 21, 2024.

12. On August 23, 2024, Special Agent Timothy Kenny submitted an affidavit and were authorized under Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A) for

[1] CW-1 has a criminal history that includes prior arrests for assault and battery with a dangerous weapon, breaking and entering, and distribution of Class A. On previous occasions, CW-1 has accurately identified, and corroborated events and individuals involved in active criminal investigations, including drug and firearm investigations. CW-1's information has led to previous search warrants, arrests, convictions, and seizures related to drugs and firearms. At the direction of law enforcement, the CW-1 has conducted controlled purchases of evidence in conjunction with criminal investigations. CW-1's cooperation is financially motivated and CW-1 is being paid for his/her services and information provided. Based on the corroboration, including recordings, I believe that CW-1's information is reliable.

information about the location of the mobile phone assigned 857-340-8128 (the "Target Phone 6"), which is believed to be utilized by GRAY. I have reviewed that previous affidavit, 24-6636 to -6637-MPK, and resulting search warrants, which are attached and incorporated herein by reference as "Exhibit A" to this affidavit.

13. I am aware, based in part on records checks of the Massachusetts Board of Probation ("BOP") and Interstate Identification Index ("III"), that GRAY has numerous prior entries on his criminal history, including convictions for Assault & Battery (with Firearm), Possession of a Firearm without a License and Carrying a Firearm with Ammunition, without a License (2019), Attempted Assault & Battery by Discharging a Firearm and Possession of a Firearm without a License (2018) and Possession of a Firearm without a Permit (two counts) and Ammunition without an FID Card (two counts) (2015). GRAY is currently on state probation for his most recent firearm-related offense until 2025.

14. Amongst GRAY's criminal history are numerous convictions for which the possible sentence would exceed one year. Namely, in or about 2019, GRAY received a sentence of 4.5 years to 5 years in state prison, for Possession of a Firearm without a License, in the Suffolk Superior Court on docket 1984CR00462.

II. Arrest Warrant Executed on August 29, 2024

15. On August 29, 2024, members of the FBI and other law enforcement officers conducted surveillance at the TARGET LOCATION. That morning, the TARGET LOCATION was surrounded when he came to the door, and GRAY was arrested by members of Boston FBI SWAT team at the TARGET LOCATION.

16. During a search of GRAY incident to arrest, investigators recovered a small bag of leafy green substance (suspected marijuana), US currency (approximately $400), and a cell phone from GRAY's pockets. GRAY asked investigators to return his cell phone and money to his family members who were inside the TARGET LOCATION. GRAY was also not wearing shoes and he asked investigators to go back inside and get his shoes for him.

17. While getting shoes for GRAY and returning the cell phone to GRAY's family members, two of the family members directed investigators to GRAY's bedroom and to leave GRAY's cell phone on his bed. Investigators went to the bedroom and observed numerous items in plain view:

a. A sentry safe, with the top lid open, on the floor of GRAY's bedroom next to the bedroom windows. Inside the safe, investigators could see a box of ammunition capable of holding fifty (50) rounds of 40 caliber bullets, three (3) loose bullets of different calibers, a clear plastic baggy containing other caliber bullets, and a tactical flashlight which I know, based on my training and experience, can be used to affix to a pistol;

b. On the dresser table, investigators observed a MASS DTA card for Jerry M GRAY, #600875137557184545;

c. Looking outside a bedroom window, investigators saw a black semiautomatic pistol magazine on the ground in the grass; and

d. Sticking out of a sweatshirt stuffed into the left side of the air conditioning unit in a bedroom window, the bottom of a black pistol grip, for what I believe based on my training & experience to be a firearm.

18. After the plain view observations were made, investigators froze the TARGET LOCATION in order to request a search warrant.

19. Based on the information provided in this affidavit, and attached in Exhibit A, I have probable cause to believe that the premises to be searched contains fruits, evidence, and instrumentalities of violations of the federal statutes listed above, as described in Attachment B.

THE PREMISES CONTAINS EVIDENCE, FRUITS, AND INSTRUMENTALITIES

20. I also have probable cause to believe that the premises to be searched contains fruits, evidence, and instrumentalities of violations of the federal statutes listed above, as described in Attachment B.

21. Through my training, experience, debriefings with drug traffickers, and consultation with other special agents and law enforcement officers, I have learned that:

a. Individuals involved in drug trafficking maintain documents and other records related to their illicit business at their residence and locations associated with them, including stash houses where they store their drugs and firearms. Specifically, individuals involved in drug trafficking and illegal firearm possession often maintain ledgers in order to keep track of the purchasing, storage, distribution, and transportation of drugs and/or the laundering of the proceeds of their drug sales. Even after the drugs are sold and/or used, documentary records and ledgers are often maintained for long periods of time to memorialize past transactions and to maintain the names, telephone numbers, and contact information for suppliers, customers, and co-conspirators. In my experience, premises used by drug traffickers (including stash houses) often contain documents and articles of personal property evidencing the identity of person(s) occupying, possessing, residing in, owning, frequenting or controlling the residence and premises;

b. Individuals involved in drug trafficking and illegal firearm possession often store controlled substances and firearms in their homes or other residences to which they have access;

c. Individuals involved in drug trafficking and illegal firearm possession commonly conceal records of drug transactions in secure locations within their cell phones, computers, residences, businesses, and/or other locations and devices over which they maintain dominion and control, for ready access and to conceal these items from law enforcement authorities;

d. Moreover, drug trafficking and individuals who illegally possess firearms commonly possess and use multiple cellular telephones simultaneously to conduct their trafficking activities, and many of these cellular telephones are kept at their residences. It is common for these cellular telephones to be retained, although not necessarily used, for months or longer by traffickers in their vehicles, residences, and businesses. Drug and firearm

traffickers often do not discard their cellular telephones immediately after they stop actively using them. Therefore, while it is common for drug traffickers to stop using cellular telephones frequently, it is far less common for drug traffickers to discard their cellular telephones after they switch to new cellular telephones. As a result, I am aware that collections of cellular phones have been found during search warrants that have included cellular phones that were no longer being used by a particular trafficker but had nevertheless been retained;

e. Individuals involved in drug trafficking and illegal firearm possession commonly have photographs of themselves, their associates, their property, and their products in their possession or in their residences, and frequently maintain these photographs on their cell phone(s) and other electronic devices;

f. Individuals involved in drug trafficking and illegal firearm possession frequently maintain the items described above inside safes, key-lock strong boxes, suitcases, safe deposit boxes and other containers, which are further secured by combination and/or key locks of various kinds in order to hide the contraband from other individuals living at or in the vicinity of their residence;

g. Individuals involved in drug trafficking and illegal firearm possession frequently build "stash" places within their residences or other locations in order to store illicit drugs as well as the items described above;

h. Individuals involved in drug trafficking keep weapons, including firearms, at the locations where they store their drug supplies in order to protect both themselves and their drugs from thefts and/or robberies; and

i. Finally, as noted above, individuals typically possess in their residences documents and other items that reflect their occupancy and control of the premises, such as but not limited to personal mail, checkbooks, identification, notes, correspondence, leases, utility bills, rent receipts, financial documents, house keys, mail keys, storage keys, and photographs.

22. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computer equipment to carry out, communicate about, and store records regarding their daily activities. These tasks are frequently accomplished through sending and receiving e-mail, instant messages, and other forms of phone or internet based

messages; scheduling activities; keeping a calendar of activities; arranging travel; purchasing items; searching for information including information regarding travel and activities; arranging for travel, accessing personal accounts including banking information; paying for items; and creating and storing images and videos of their movements and activities.

23. Based on my training and experience, and information provided to me by other agents, I know that individuals who illegally distribute controlled substances commonly use cellular telephones to communicate about and further their illegal activities. They use their cellular phones in order to communicate with suppliers, potential buyers, or other individuals potentially involved in unlawful business transactions and will maintain information about these individuals in their contacts lists, in saved text messages and in other places. These communications occur in a variety of ways, which include, but are not limited to: text messaging (often used in lieu of phone calls to avoid speaking over the telephone), and messaging through applications such as Snapchat, WhatsApp, and Facebook.

24. Based on my training, experience, and information provided by other Agents, I know that many smartphones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

25. Based upon my knowledge, training and experience, I know that a cellular telephone is a handheld wireless device used primarily for voice communication through radio

signals. These telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; maintaining travel documents, including boarding passes; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. Based on my training and experience, I know that many cellular telephones have the capabilities described above.

26. As described above, the investigation has uncovered evidence that GRAY, and others yet unknown, used their cellular phones during the commission of the offenses, to arrange drug deals with customers. Based on my experience and training, I know that records relating to these communications, including text messages, are likely stored on these phones.

27. Seizure of devices containing this information will provide information relating to coconspirators and accomplices. I know, based upon my training and experience, as well as consultation with other investigators, that individuals who sell illegal drugs typically use cellular telephones to communicate with their suppliers, their customers, and with other coconspirators, and that they communicate both via voice calls and via email and/or text messaging. I also know

that persons who sell illegal drugs regularly keep records of their illegal activities. These records can include, but are not limited to, contact lists of buyers and sellers, ledgers of sales and money owed by customers or to suppliers, and lists of quantities and/or specific controlled substances preferred by or ordered by specific customers. Individuals engaged in drug trafficking often take photographs of their closest confederates. Records of drug trafficking can be produced and maintained on paper in a tangible form and/or by electronic means on cellular telephone, electronic/digital storage device and/or a computer. In the case of electronic or digital media, the information can be maintained on the device itself or on portable digital storage media, making it easier to conceal. From my training, experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment B on their cellular telephones.

28. As with most electronic/digital technology items, communications made from an electronic device, such as a computer or a cellular phone, are often saved or stored on the device. Storing this information can be intentional, for example, by saving an e-mail as a file on a computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication or of an internet search may be automatically stored in many places on a computer or a cell phone. In addition to electronic communications, a user's Internet activities generally leave traces in the web cache and Internet history files. A forensic examiner often can recover evidence that shows when and in what manner a user of an electronic device, such as a computer or a cell phone, used such a device.

29. Additionally, many cellular phones today have a GPS navigation device on the

phone. Examination of the GPS data on a cellular phone can provide valuable evidence as to the locations where drug traffickers meet with coconspirators, including their sources of supply, and can aid in identifying those individuals. Additionally, review of GPS data can aid in identifying offsite locations where drug traffickers store drugs, maintain bank accounts, and conceal their drug proceeds.

30. I believe that the TARGET LOCATION may contain telephone devices that can only be unlocked with a fingerprint or via facial recognition. For example, I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones, offer their users the ability to unlock the device via the use of a fingerprint in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to five fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a passcode, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

31. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode must be used instead, such as: (1) when more than 48 hours has

passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

32. I am also aware that more recent Apple products no longer use Touch ID and instead use a security feature called Apple Face ID. Apple Face ID is a facial recognition system that uses the phone's camera to scan the face of the user and, if the scan matches the data on file, performs actions like unlocking the phone.

33. The passcodes that would unlock these devices are not known to law enforcement. Thus, it may be necessary to press the fingers of the users of the devices to the device's Touch ID sensor or use the device's camera to access Face ID in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock devices with the use of the fingerprints of the users or use the device's camera and take a scan of the user is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

34. Based on the facts discussed in this affidavit, I am asking for authorization to place the fingerprints of the individuals who have been known to use certain telephones to unlock the device via Touch ID, or use of the device's camera to scan that individual's face to unlock the device via Face ID. I intend to call each of the telephone numbers specified in the Attachment B corresponding to the TARGET LOCATION when searching the TARGET LOCATION. If the

phone rings, and the user is present, I request authority to place his or her fingers on the Touch ID sensor, if one exists, to unlock the devices and/or use the camera on the device to scan either that individual's face to unlock the phone using Face ID.

35. In sum, I have participated in the execution of numerous search warrants at the residences and stash locations of similar to the targets of this investigation. In a substantial number of residential searches executed in connection with the investigations in which I have been involved, the following types of evidence typically have been recovered in both conventional and electronic formats:

a. controlled substances;

b. weapons, including firearms, at the locations where they store their drug supplies in order to protect both themselves and their drugs from thefts and/or robberies;

c. paraphernalia for packaging, processing, diluting, weighing, and distributing controlled substances, such as scales, funnels, sifters, grinders, glass panes and mirrors, razor blades, plastic bags, microwave ovens, heat-sealing devices, and diluents such as mannitol, mannite, and inositol;

d. books, records, receipts, notes, ledgers, letters, and other papers relating to the distribution of controlled substances, travel for the purpose of acquiring and/or distributing controlled substances, and to monetary transactions involving the proceeds from the sale of controlled substances;

e. personal books, papers, and other electronic devices reflecting names, addresses, telephone numbers, and other contact or identification data relating to the distribution of controlled substances, money laundering, and the criminal use of communication facilities;

f. cash, currency, and records relating to the generation of income from the sale of controlled substances and the expenditure of such income, including money orders, wire transfers, cashier's checks and receipts, bank statements, passbooks, checkbooks, and check registers, as well as consumer items such as electronic equipment, vehicles, jewelry, and precious metals such as gold and silver, and precious gems such as diamonds - it should be noted that possession of the valuable items referenced in this paragraph, particularly by

individuals with no substantial legitimate source of income, is evidence of drug trafficking as opposed to drug use;

g. documents and other records indicating travel in interstate and foreign commerce, such as maps, GPS coordinates, navigation coordinates, travel itineraries, plane tickets, boarding passes, motel and hotel receipts, passports and visas, credit card receipts, and telephone bills and related communications;

h. cellular telephones, smart phones, electronic tablet devices, and other electronic media utilized for communication, transportation, and data acquisition and retention purposes related to acquiring and distributing illegal drugs and proceeds, including incoming and outgoing call and text message logs, contact lists, photo and video galleries, sent and received text messages, online searches and sites viewed via the internet, online or electronic communications sent and received (including email, chat, and instant messages), sent and received audio files, navigation, mapping, and GPS files, telephone settings (including contact lists) text messages, and related identifying information such as telephone identification numbers, call forwarding information, messages drafted but not sent, and voice messages;

i. identification evidence and/or indicia, such as cell phones with particular numbers, mail, deeds, leases, rental agreements, photographs, bills, and identification documents, that tend to identify the person(s) in residence, occupancy, control, or ownership of subject premises and/or subject communication devices;

j. Firearms, explosives, ammunitions, firearm components, firearm accessories, tactical equipment and other items pertaining to the domestic and international trafficking of firearms, including, but not limited to, handguns, pistols, revolvers, rifles, machine guns, and other weapons, and any records of receipts pertaining to firearms, parts, accessories and ammunition;

k. Any and all tools reasonably believed to be possessed or used by subject of this investigation in furtherance of manufacturing or modifying firearms; including but not limited to drills, presses, jigs, and cutting tools.

l. Records and documents showing indicia of residency;

m. Books, records, receipts, bills of lading, notes, ledgers, papers, business records, packaging, and other items relating to the purchase, possession,

receipt, transfer, manufacture or distribution of firearms, including, but not limited to, materials, chemicals, tools and literature related to firearms;

n. Wireless telephones, telephone bills, telephone note pads and notes, contracts and other documents reflecting the ownership, subscription information, and the use of the telephones, reasonably believed to be possessed or used by subject of this investigation in furtherance of the Target Offenses;

o. Photographs, including still photographs, negatives, video recordings, slides, film, undeveloped film, digital photos and the contents therein, in particular, photographs of co-conspirators, or those relating to purchase, possession, receipt, transfer, manufacture or distribution of firearms;

p. Contact information relating to suppliers, manufacturers and purchasers involved in the purchase, possession, receipt, transportation, transfer, manufacture or distribution of firearms;

q. Correspondence pertaining to the purchase, possession, receipt, transfer, manufacture or distribution of firearms, whether transmitted or received using a computer, wireless telephone, a facility or means of interstate commerce, common carrier, or mail; and

r. Safes or other locked containers and their contents to be searched for the listed items.

36. Based on my knowledge, training, experience, and information provided to me by other agents, I know that data can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

CONCLUSION

37. Based on the information described above, I have probable cause to believe that GRAY and others yet unknown unknown, have violated federal law, including Title 21 U.S.C. § 841(a)(1) (possession with intent to distribute, and distribution of, controlled substances) and Title 18 U.S.C. § 922(g)(1) (being a felon in possession of a firearm and ammunition).

38. Based on the information described above, I also have probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in Attachment B, are contained within the premises described in Attachment A.

Sworn to under the pains and penalties of perjury,

/s/ John P. Farley

John P Farley
Special Agent, FBI

Signed electronically and sworn to via telephone in accordance with Federal Rule of Criminal Procedure 4.1 on this __ day of August, 2024.

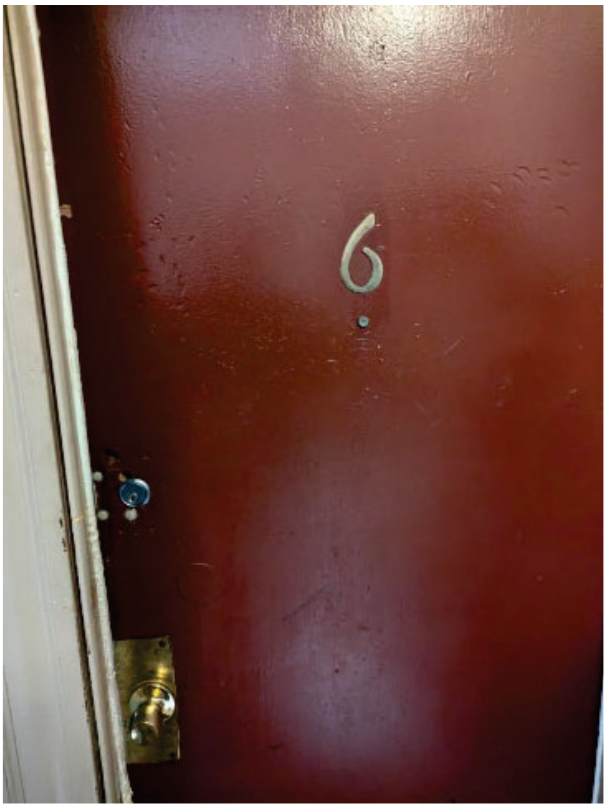
August 29, 2024

HON. M. PAGE KELLEY
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF MASSACHUSETTS

ATTACHMENT A

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The premises to be searched is located at 28 Deckard Street, Apt #6, Roxbury, MA (the "TARGET LOCATION"). The building at 28 Deckard Street is a brick multi-unit apartment building, with the number "28" above the door. Apartment 6 is located on the 2nd floor. The maroon door to Apartment 6 has a gold door handle and the number "6" affixed to the middle of the door. Photos of 28 Deckard Street, Apt #6 are below:



The premises to be searched shall include all common areas, rooms, crawl spaces, storage areas, and containers such as safes, vaults, file cabinets, drawers, backpacks, luggage, briefcases, valises, boxes, jewelry boxes, cans, bags, purses, and trash cans, located in or around the TARGET LOCATION, that are owned or under the control of the occupants of the TARGET LOCATION.

ATTACHMENT B

ITEMS TO BE SEIZED

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) and 18 U.S.C. § 922(g)(1) for the period of February 1, 2024 through the present day, including:

A. Controlled substances;

B. Records and tangible objects pertaining to the following people, entities, physical addresses, and telephone numbers:

1. JERRY GRAY ("GRAY"), DOB: xx/xx/1996

C. Records and tangible objects pertaining to:

1. drug trafficking, and other related crime in furtherance of drug trafficking offenses;

D. Records and tangible objects pertaining to the payment, receipt, transfer, or storage of money or other things of value by GRAY or any one of the names listed above, including, without limitation:

1. Bank, credit union, investment, money transfer, and other financial accounts;

2. Credit and debit card accounts;

3. Tax statements and returns;

4. Business or personal expenses;

5. Income, whether from wages or investments;

6. Loans;

E. Records and tangible objects pertaining to the travel or whereabouts of by

GRAY between February 1, 2024 through the present day;

F. Records and tangible objects pertaining to the existence, identity, and travel of any co-conspirators, as well as any co-conspirators acts taken in furtherance of the crimes listed above;

G. Records and tangible objects pertaining to;

1. Documents and items reflecting or memorializing the manufacturing, ordering, possession, purchase, storage, distribution, and/or transportation of controlled substances, including communications, records of sales, records of purchases, log books, drug ledgers, personal telephone/address books containing the names of purchasers and suppliers of controlled substances used to manufacture controlled substances, electronic organizers, Rolodexes, telephone bills, telephone answering pads, bank and financial records, and storage records, such as storage locker receipts, storage locker keys, and safety deposit box rental records and keys;

2. Documents and articles of personal property reflecting the identity of persons occupying, possessing, residing in, owning, frequenting or controlling the premises to be searched or property therein, including keys, rental agreements and records, property acquisition records, utility bills and receipts, photographs, answering machine tape recordings, telephones, vehicle and/or vessel records, canceled mail envelopes, correspondence, financial documents such as tax returns, bank records, safety deposit box records, canceled checks, and other records of income and expenditure, credit card records, travel documents, clothing, and personal identification documents;

3. Photographs, video, and audio recordings which document an association with other co-conspirators and/or which display controlled substances, firearms, or chemicals/materials used in the manufacturing of controlled substances;

4. Materials, equipment and paraphernalia associated with the manufacturing, ordering, possession, purchase, storage, distribution, and/or transportation of controlled substances, including, but not limited to, packaging materials, storage bins, containers, cutting agents, and scales;

5. Firearms, firearms accessories, body armor, and ammunition or other dangerous weapons associated with the protection of drug trafficking, and any such documents relating to the purchase and/or possession of such items;

6. Items indicative of unexplained wealth or evidencing the proceeds derived from illicit drug trafficking, including but not limited to large sums of money, expensive vehicles, financial instruments, precious metals, jewelry, and real estate, and documents evidencing the procuring or leasing of these items;

H. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;

4. evidence of counter-forensic programs and associated data that are designed to eliminate data;

5. evidence of when the computer equipment was used;

6. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment; and

7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage;

I. Records and tangible objects relating to the ownership, occupancy, or use of the premises to be searched (such as utility bills, phone bills, rent

payments, mortgage payments, photographs, insurance documentation, receipts and check registers).

II. All computer hardware, computer software, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

III. During the execution of the search of the Subject Premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the Subject Premises to the sensor of the subject device and/or to hold the device in front of their faces.

DEFINITIONS

For the purpose of this warrant:

A. "Computer equipment" means any computer hardware, computer software, mobile phone, storage media, and data.

B. "Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cell/mobile phone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility,

communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files

that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes.